UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/485,352	03/13/2000	Michael DUPRE	2643/OG629	1819

7590 12/23/2003

Christa Hildebrand
NORRIS, McLAUGHLIN & MARCUS, P.A.
220 East 42nd Street
30th Floor
NEW YORK, NY 10017

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	10

DATE MAILED: 12/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/485,352	DUPRE, MICHAEL	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-19* is/are pending in the application.

4a) Of the above claim(s) *1-13* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. This action is responsive to communication: original application filed 14 March 2000 with a foreign priority date of 4 August 1997.C

2. Claims 1-13 withdrawn from consideration indicated in pre-amendment, 4 February 2000.

3. Claims 14-22 are currently pending in this application. Claims 14 and 19 are independent claims.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5. **Claims 14-22** are rejected under 35 U.S.C. 102(e) as being anticipated by Brown et al. U.S. Patent No. 5,793,866 (hereinafter '866).

6. **As to independent claim 14,** "A method for personalizing GSM chips" is disclosed in '866 col. 1, lines 27-30 and col. 2 lines 31-33 -33 (i.e. 'subscriber device' or 'remote device') "Protocols for authentication exist in many systems. For example, cellular systems, including the Global System for Mobile Communications (GSM)" and "A system and method of improving communication link security allows the subscriber

device to verify reception of a first signal, which is at least a component of a public key, transmitted between a central site and a remote device";

- "having a memory range in which is taught in '866 col. 3, lines 55-60 "A memory circuit 156 is connected to controller 142 via data bus 158. The memory stores an operating program for the controller and secure information received from the central site 102";

- "at least one Subscriber identification number IMS1 and a card number ICCID are stored" is taught in col. 4 17-18 "For this purpose, a telephone number and subscription ID are stored in the remote device";

- "wherein for personalizing the chip an additional secret key Ki and, optionally, additional data are stored, wherein at the manufacturer for pre-personalizing the chip, at least initial card specific data, namely a first secret key Ki_1 and, optionally, additional data, such as PIN and PUK are stored, comprising the steps of" is disclosed in '866 col. 4 lines 53-63 "With reference to FIG. 3, once the base station 202 recognizes the special-purpose call on the control channel, the potential subscriber is routed through a voice channel to the service provider to exchange OTA messages between the service provider central site 102 and the mobile subscriber remote device 104. In a Rivest, Shamir, Adleman (RSA) embodiment, the public-key modulus N1 is transmitted to the remote device 104 from the service provider controller 108. N1 is the public modulus, and it is the product of P1 and Q1, two secret numbers stored in the memory 114 and having a known criteria";

- "a) performing the personalization of the chip when the subscriber logs on to the subscriber network for the first time" is shown in '866 col. 4, lines 15-53 "Activation of the remote device 104 includes associating the electronic serial number, or address, with a particular subscriber ... The service provider, a central site, can also include a home location register (HLR), an authentication center (AC) and an over-the-air functionality (OTAF) for over-the-air service provisioning. ... This remote device can originate a special purpose call to any of several service providers (such as service provider central site 102) to request activation";

- "b) obtaining the ICCID and the IMS1 from a number pool, the chip itself derives an initial key Ki_1 from a key K1 which is known and entered into the chip" is disclosed in col. 4 lines 63-67 "The remote device 104 responds to the modulus N1 by generating a ciphertext number C, which is a function of the modulus N1, a random number n generated by the remote device 104, and an arbitrary number e. The value of e is known to both the remote device 104 and the central site 102";

- "while PIN and PUK are set to a default value" is shown in '866 col. 4 line 63 "it is the product of P1 and Q1, two secret numbers stored in the memory 114 and having a known criteria";

- "c) making an entry in the authentication center (AC) and the home location register (HLR) as soon as a subscriber has entered into a contract with the network operator" is taught in '866 col. 4, lines 39-47 "The service provider, a central site, can also include a home location register (HLR), an authentication center (AC) and an over-the-air functionality (OTAF) for over-the-air service provisioning. It has become

desirable for over-the-air service provisioning to provide the subscription ID to the remote device 104, a mobile subscriber in the cellular system. This allows the subscription ID to be down-loaded from the central site 102, the service provider facility, to the subscriber remote device 104";

- "d) deriving the authentication center (AC) the initial first key Ki_1" is shown in col. 5 lines 2-4 "When the ciphertext number C is received by the service provider, it is decoded using the equation n=C.sup.d1 mod N1, to determine n";

- "e) setting the conditions of the network so that during logon to the network, a connection is established from the chip to the security center of the network operator (SC)" col. 4 lines 29-33 "A base station 202 (FIG. 2) is connected to a remote device 104 (a cellular telephone) through a communication link 105, which is an RF wireless link. The base station is in turn connected to the service provider central site 102 through a mobile switching office, or center, 206. A local public switched telephone network (PSTN) 208 is also connected to the mobile switching center 206";

- "f) routing the connection from the chip to the SC during the first logon" is disclosed in col. 4 lines 53-55 "With reference to FIG. 3, once the base station 202 recognizes the special-purpose call on the control channel, the potential subscriber is routed through a voice channel to the service provider to exchange OTA messages between the service provider central site 102 and the mobile subscriber remote device 104";

- "g) negotiating a new second secret key Ki_2" is taught in col. 5 lines 4-8 "The random number n is subsequently used to encrypt the authentication key, otherwise

known as the A-key. The encrypted A-key is communicated to the remote device 104 from the service provider central site 102";

- "optionally, a PUK with the chip or generated in the security center (SC) and transmitted to the chip" is shown in col. 5, lines 8-13 "Once the A-key is known to both parties, a series of messages are then exchanged between the central site 102 and the remote device 104 by which a security related variable called shared secret data (SSD) is mutually calculated by both the remote device 104 and the service provider central site 102";

- "h) disabling the conditions of step e)" is taught in col. 6 lines 19-23 "If the numbers do not match, the OTASP process is aborted. This provides security since it will be difficult for the intruder to continue operating between remote device 104 and central site 102 and to mimic the voice of the subscriber without introducing a substantial delay period".

6. **As to dependent claim 15,** "wherein the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the AC before the contract is established" is taught in '866 col. 4, lines 47-49 "the OTASP protocol, a subscriber purchases a "blank" remote device, which is a remote device having no subscription ID. This remote device can originate a special purpose call to any of several service providers (such as service provider central site 102) to request activation".

7. **As to dependent claim 16,** "The method according to claim 14, further comprising the step of employing a Diffie Hellman method to negotiate the second secret key Ki_2 is shown in '866 col. 10 lines 9-15 "Those skilled in the art will recognize

that the above RSA public key cryptography examples are not restrictive, as the methods disclosed may be applied to other techniques. For example, the methods may also be used to provide improved security in Diffie-Hellman (DH) public key cryptography. In DH techniques, a pair of signals are exchanged between the central site".

8. **As to dependent claim 17,** "wherein the home location register (HLR) is capable of setting and deleting a rerouting command (hotlining flag) is disclosed in '866 col. 6 lines 15-23 "The controller 108 of the central site 102 likewise generates a number for display 118 having the same relationship to the modulus N1. The user can then read the characters on the display 148 to the service provider operator, who is simultaneously reading the display 118. If the numbers do not match, the OTASP process is aborted. This provides security since it will be difficult for the intruder to continue operating between remote device 104 and

central site 102 and to mimic the voice of the subscriber without introducing a substantial delay period".

9. **As to dependent claim 18,** "wherein, when the initial key Ki_1 is entered into the authentication center (AC) for the first time, the hotlining flag is also set in the home location register (HLR) is taught in '866 col. 4 lines 39-60 "The service provider, a central site, can also include a home location

register (HLR), an authentication center (AC) and an over-the-air functionality (OTAF) for over-the-air service provisioning ... his remote device can originate a special purpose call to any of several service providers (such as service provider

central site 102) to request activation ... the public-key modulus N1 is transmitted to the remote device 104 from the service provider controller 108. N1 is the public modulus, and it is the product of P1 and Q1, two secret numbers stored in the memory 114 and having a known criteria".

10. **As to independent claim 19** cites the same text as claim 14 and is rejected using the same rationale.

11. **As to dependent claim 20,** "The chip according to claim 19, wherein the chip includes means for receiving data from the security center (SC) and means for writing these data to a memory and, optionally, reading these data from the memory, changing these data and/or transmitting these data to the security center (SC) is shown in '866 col. 4, lines 15-55 "The service provider, a central site, can also include a home location register (HLR), an authentication center (AC) and an over-the-air functionality (OTAF) for over-the-air service provisioning. It has become desirable for over-the-air service provisioning to provide the subscription ID to the remote device 104, a mobile subscriber in the cellular system. This allows the subscription ID to be down-loaded from the central site 102, the service provider facility, to the subscriber remote device 104 ... With reference to FIG. 3, once the base station 202 recognizes the special-purpose call on the control channel, the potential subscriber is routed through a voice channel to the service provider to exchange OTA messages between the service provider central site 102 and the mobile subscriber remote device 104. In a Rivest, Shamir, Adleman (RSA) embodiment, the public-key modulus N1 is transmitted to the remote device 104 from the service provider controller 108. N1 is the public modulus,

and it is the product of P1 and Q1, two secret numbers stored in the memory 114 and having a known criteria. The remote device 104 responds to the modulus N1 by generating a ciphertext number C, which is a function of the modulus N1, a random number n generated by the remote device 104, and an arbitrary number e. The value of e is known to both the remote device 104 and the central site 102. The response C is sent from the device to the service provider ".

12. **As to dependent claim 21, "**The chip according to claim 20, wherein the chip comprises a microprocessor for negotiating a secret key with the security center (SC) is disclosed in '866 col. 3, lines 48-50 "The controller 142 can be implemented using a microprocessor, a digital signal processor, a microcomputer, or the like. The controller 142 is coupled to a display 148 via a bus 149".

13. **As to dependent claim 22,** "The chip according to claim 21, wherein the chip includes a dialing number which is fixedly programmed by the manufacturer (fixed dialing) is taught in '866 col. 4 lines 15-18 "Activation of the remote device 104 includes associating the electronic serial number, or address, with a particular subscriber. For this purpose, a telephone number and subscription ID are stored in the remote device".

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Nevoux et al	U.S. Patent No. 5,661,806 issued dated: Aug. 26, 1997
Sudia	U.S. Patent No. 5,799,086 issued dated: Aug. 25, 1998

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Ellen Tran
Patent Examiner
Technology Center 2134
11 December 2003